

IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Previously Presented): A transmitter device which transmits first data to a receiver device by driving a recording medium that stores the first data and second data that describes a limitation on the usage of the first data, the transmitter device comprising:

storage means for storing a check value calculated on the basis of the second data;

communication means which, in the authenticating of the receiver device, transmits the second data to the receiver device and receives a check value calculated on the basis of the second data from the receiver device; and

determination means which, in the authenticating of the receiver device, determines whether the check value of the second data received by the communication means matches the check value of the second data stored in the storage means.

Claim 2 (Previously Presented): A transmitter device according of Claim 1, wherein the storage means inhibits the writing or reading of the check value of the second data in a process other than the authentication process.

Claim 3 (Previously Presented): A transmitter device according to Claim 1, wherein the storage means is tamper resistant.

Claim 4 (Previously Presented): A transmitting method of a transmitter device which transmits first data to a receiver device by driving a recording medium that stores the first data and second data that describes a limitation on the usage of the first data, the transmitting method comprising:

a step of storing a check value calculated on the basis of the second data;

in an authenticating step of the receiver device, a step of communication for transmitting the second data to the receiver device and for receiving a check value calculated on the basis of the second data from the receiver device; and

in the authenticating of the receiver device, a step of determining whether the check value of the second data received in the communication step matches the check value of the second data stored in the storing step.

Claim 5 (Previously Presented): A program storage medium for storing a transmission process program for transmitting first data to a receiver device by driving a recording medium that stores the first data and second data that describes a limitation on the usage of the first data, the program executed by a transmitter device and comprising:

a step of storing a check value calculated on the basis of the second data;

in an authenticating step of the receiver device, a step of communication for transmitting the second data to the receiver device and for receiving a check value calculated on the basis of the second data from the receiver device; and

in the authenticating of the receiver device, a step of determining whether the check value of the second data received in the communication step matches the check value of the second data stored in the storing step.

Claim 6 (Previously Presented): A receiver device for receiving first data from a transmitter device, the receiver device comprising:

communication means which, in the authenticating of the transmitter device, receives, from the transmitter device, second data that describes a limitation on the usage of the first data and transmits a check value calculated on the basis of the second data to the transmitter device; and

encrypted value generator means for generating the check value of the second data based on the second data received by the communication means, in the authenticating of the transmitter device, said check value for detecting whether the second data has been tampered with or not.

Claim 7 (Previously Presented): A receiver device according to Claim 6, further comprising

random number generator means for generating a random number having a predetermined bit number, wherein the communication means transmits, to the transmitter device, the check value of the second data together with the random number generated by the random number generator means.

Claim 8 (Previously Presented): A receiver device according to Claim 6, further comprising usage limiting data generator means which generates, subsequent to the reception of the first data, third data which describes a limitation on the usage of the first data, based on the second data received by the communication means,

wherein the encrypted value generator means generates a check value generated on the basis of the third data generated by the usage limiting data generator means, and

the communication means transmits, to the transmitter device, the check value of the second data together with the check value of the third data.

Claim 9 (Previously Presented): A receiving method of a receiver device for receiving first data from a transmitter device, comprising:

in the authenticating of the transmitter device, a step of communication for receiving, from the transmitter device, second data that describes a limitation on the usage of the first

data and for transmitting a check value calculated on the basis of the second data to the transmitter device; and

in the authenticating of the transmitter device, a step of generating a check value of the second data based on the second data received in the communication step, said check value for detecting whether said second value has been tampered with or not.

Claim 10 (Previously Presented): A program storage medium for storing a reception process program for receiving first data from a transmitter device, the program executed by a receiver device and comprising:

in the authenticating of the transmitter device, a step of communication for receiving, from the transmitter device, second data that describes a limitation on the usage of the first data and for transmitting a check value calculated on the basis of the second data to the transmitter device; and

in the authenticating of the transmitter device, a step of generating a check value of the second data based on the second data received in the communication step, said check value for detecting whether said second value has been tampered with or not.

Claim 11 (Previously Presented): A communication system comprising a transmitter device which transmits first data by driving a recording medium that stores the first data and second data that describes a limitation on the usage of the first data, and a receiver device for receiving the first data;

the transmitter device comprising:

storage means for storing a check value calculated on the basis of the second data;

first communication means which, in the authenticating of the receiver device, transmits the second data to the receiver device and receive a check value calculated on the basis of the second data from the receiver device; and

determination means which, in the authenticating of the receiver device, determines whether the check value of the second data received by the communication means matches the check value of the second data stored in the storage means; and

the receiver device comprising:

second communication means which, in the authenticating of the transmitter device, receives, from the transmitter device, second data that describes a limitation on the usage of the first data and transmits the check value calculated on the basis of the second data to the transmitter device; and

encrypted value generator means for generating the check value of the second data based on the second data received by the communication means, in the authenticating of the transmitter device, said check value for detecting whether the second data has been tampered with or not.

Claims 12-25 (Canceled).